PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2003-006164**
(43)Date of publication of application : **10.01.2003**

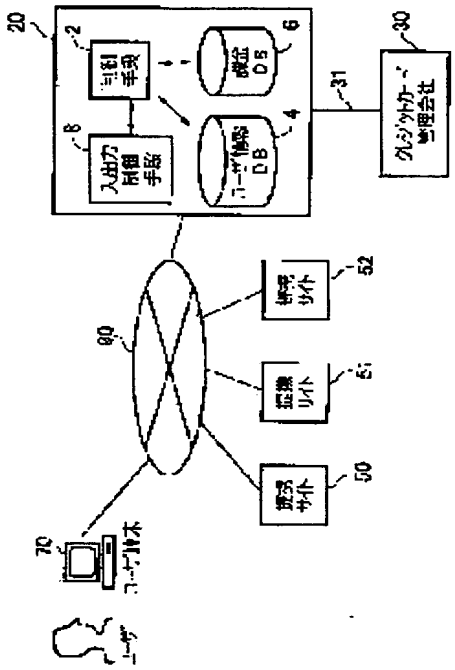
(51)Int.Cl. **G06F 15/00**
G06F 17/60

(21)Application number : **2001-188022**
(22)Date of filing : **21.06.2001**

(71)Applicant : **AOKI NORIYASU**
(72)Inventor : **AOKI NORIYASU**

(54) SYSTEM AND METHOD FOR AUTHENTICATION AND COMPUTER PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an authentication system and an authenticating method, capable of representatively authenticating a user accessing an affiliated site, and to provide a computer program.
SOLUTION: This authentication system 20 is provided with a user information database 4 connected to affiliated sites 50 to 52 on a Web via a network 90 and storing authentication information of users which has been allowed to access the affiliated sites and a control means 2 for acquiring authentication information inputted to the affiliated sites, performing authentication processing on the basis of the user information database and transmitting authentication the results to the affiliated sites.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁(JP)　(12)公開特許公報（A）　(11)特許出願公開番号

特開２００３－６１６４
（Ｐ２００３－６１６４Ａ）
(43)公開日　平成15年1月10日(2003.1.10)

(51)Int.Cl.⁷		識別記号	F I			テーマコード(参考)
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ	15/00	３３０　Ｂ	5B085
	17/60	１４０		17/60	１４０	
		４１４			４１４	
		５０４			５０４	
		ＺＥＣ			ＺＥＣ	

審査請求　未請求　請求項の数６　ＯＬ　（全６頁）

(21)出願番号　特願2001-188022(P2001-188022)

(22)出願日　平成13年6月21日(2001.6.21)

(71)出願人　501249582
青木　規安
千葉県松戸市新松戸4－11　メゾン・ド・ココット303

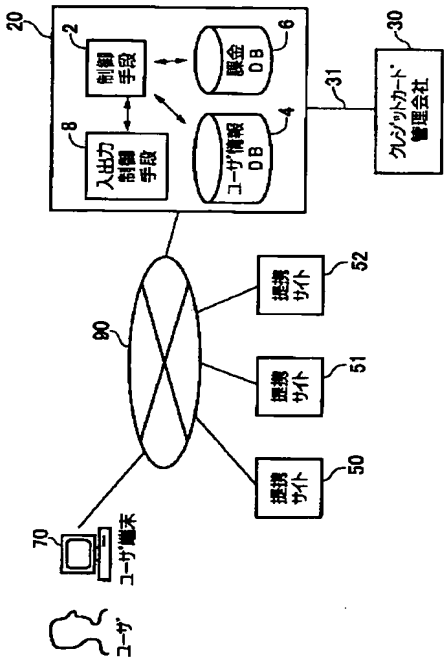
(72)発明者　青木　規安
千葉県松戸市新松戸4－11　メゾン・ド・ココット303

(74)代理人　100064908
弁理士　志賀　正武　（外6名）

Ｆターム(参考)　5B085 AE02 AE03 BA07 BC01 BG03 BG07

(54)【発明の名称】認証システム及び認証方法、並びにコンピュータプログラム

(57)【要約】
【課題】　提携サイトにアクセスするユーザの認証を代行可能な認証システム及び認証方法、並びにコンピュータプログラムを提供する。
【解決手段】　Ｗｅｂ上の提携サイト５０～５２とネットワーク９０を介して接続され、提携サイトへのアクセスが許容されたユーザの認証情報を格納するユーザ情報データベース４と、提携サイトへ入力された認証情報を取得し、ユーザ情報データベースに基づいて認証処理を行い、認証結果を提携サイトへ送信する制御手段２とを備えた認証システム２０である。



1

【特許請求の範囲】

【請求項１】　Ｗｅｂ上の提携サイトとネットワークを介して接続され、
前記提携サイトへのアクセスが許容されたユーザの認証情報を格納するユーザ情報データベースと、
前記提携サイトへ入力された認証情報を取得し、前記ユーザ情報データベースに基づいて認証処理を行い、認証結果を前記提携サイトへ送信する制御手段とを備えたことを特徴とする認証システム。

【請求項２】　前記制御手段は、前記認証結果に関連付けて前記ユーザの呼称情報を送信することを特徴とする請求項１に記載の認証システム。

【請求項３】　前記制御手段は、前記提携サイトへのアクセスを希望するユーザの申請したクレジットカード番号が、該クレジットカードの管理会社により認証された場合に、前記ユーザの認証情報を発行することを特徴とする請求項１又は２に記載の認証システム。

【請求項４】　前記制御手段は、前記提携サイトからの認証依頼の頻度に応じて、課金情報を記録することを特徴とする請求項１ないし３のいずれかに記載の認証システム。

【請求項５】　Ｗｅｂ上の提携サイトへのアクセスが許容されたユーザの認証情報を格納する過程と、
前記提携サイトへ入力された認証情報を取得する過程と、
前記格納された認証情報に基づいて認証処理を行い、認証結果を前記提携サイトへ送信する過程とを有することを特徴とする認証方法。

【請求項６】　Ｗｅｂ上の提携サイトへのアクセスが許容されたユーザの認証情報を格納する過程と、
前記提携サイトへ入力された認証情報を取得する過程と、
前記格納された認証情報に基づいて認証処理を行い、認証結果を前記提携サイトへ送信する過程とをコンピュータに実行させることを特徴とするコンピュータプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、Ｗｅｂ上でユーザの認証を行う認証システム及び認証方法、並びにコンピュータプログラムに関する。

【０００２】

【従来の技術】近年、インターネットの普及に伴い、いわゆるネットオークション等が盛んになっている。ところで、このネットオークションにおいては売り手と買い手の間で金銭の授受があることから、オークション参加者から所定の参加料を徴収することで、不正な者による料金未払いや商品未発送等を抑止している。

【０００３】

【発明が解決しようとする課題】しかしながら、かかる

2

参加料を徴収したとしても、やはり料金未払いや商品未発送を完全に防止することは困難である。また、いちいち参加料を徴収していては、善意の者の参加を促進することができないという問題がある。従って、安全で信頼できるユーザかどうかを認証して、このユーザのみをオークションに参加させることができれば好ましい。

【０００４】一方で、Ｗｅｂ上の仮想店舗では、商品購入時にユーザにクレジットカード番号等の入力を要求し、認証を自己のサイト内で行っている。しかし、かかる認証を個々のＷｅｂサイトすべてに課すことは、システムコストの点から困難な場合が多い。特に、運営費用の少ないサイトにとっては負担が大きく、このようなことから安価かつ容易に本人認証を行う技術が望まれている。

【０００５】本発明は、上記した問題点に鑑みてなされたもので、提携サイトにアクセスするユーザの認証を代行可能な認証システム及び認証方法、並びにコンピュータプログラムを提供することを目的とする。

【０００６】

【課題を解決するための手段】上記した目的を達成するために、請求項１記載の認証システムは、Ｗｅｂ上の提携サイトとネットワークを介して接続され、前記提携サイトへのアクセスが許容されたユーザの認証情報を格納するユーザ情報データベースと、前記提携サイトへ入力された認証情報を取得し、前記ユーザ情報データベースに基づいて認証処理を行い、認証結果を前記提携サイトへ送信する制御手段とを備えたことを特徴とする。

【０００７】前記制御手段は、前記認証結果に関連付けて前記ユーザの呼称情報を送信することが好ましい。

【０００８】前記制御手段は、前記提携サイトへのアクセスを希望するユーザの申請したクレジットカード番号が、該クレジットカードの管理会社により認証された場合に、前記ユーザの認証情報を発行することが好ましい。

【０００９】前記制御手段は、前記提携サイトからの認証依頼の頻度に応じて、課金情報を記録することが好ましい。

【００１０】本発明の認証方法は、前記提携サイトへのアクセスが許容されたユーザの認証情報を格納する過程と、前記提携サイトへ入力された認証情報を取得する過程と、前記格納された認証情報に基づいて認証処理を行い、認証結果を前記提携サイトへ送信する過程とを有することを特徴とする。

【００１１】本発明のコンピュータプログラムは、前記提携サイトへのアクセスが許容されたユーザの認証情報を格納する過程と、前記提携サイトへ入力された認証情報を取得する過程と、前記格納された認証情報に基づいて認証処理を行い、認証結果を前記提携サイトへ送信する過程とをコンピュータに実行させることを特徴とする。

【００１２】
【発明の実施の形態】以下、本発明の実施の形態について、各図を参照して説明する。図１は、本発明にかかる認証システム（以下、適宜「認証サイト」という）２０の一実施の形態を示す構成ブロック図であり、システム全体を制御する制御手段２、詳しくは後述するユーザ情報データベース（以下、適宜「ＤＢ」という）４、課金情報データベース６、ネットワーク９０との情報の送受信を行う入出力制御手段８を備えている。制御手段２は所定の中央演算処理装置（ＣＰＵ）等からなり、又、認証システム２０は全体としてＷｅｂサイトを構成している。
【００１３】認証サイト２０はネットワーク９０に接続され、当該ネットワーク９０を介してユーザ端末７０、及び提携サイト５０～５２と接続されている。また、クレジットカード管理会社３０と専用回線３１を介して接続されている。提携サイト５０～５２はＷｅｂサイトであり、アクセスを許容した所定のユーザに対し、コンテンツを閲覧させるようになっている。なお、提携サイトは、アクセス制限をせずに一般ユーザに閲覧させるコンテンツをさらに備えていてもよい。
【００１４】ここで、ユーザ端末７０は、パーソナルコンピュータ、携帯電話機やＰＨＳ（Personal Handyphone System：登録商標）、あるいはＰＤＡ（Personal DigitalAssistants：個人用情報機器）等であり、いずれもネットワーク９０に接続可能で、Ｗｅｂページを閲覧可能なブラウザが搭載されている。また、クレジットカード管理会社３０は、ユーザのクレジットカードの発行・管理を行うサーバであり、ユーザのクレジットカード情報に基づいて認証処理を行う。
【００１５】ネットワーク９０としては、インターネットの代わりに、専用回線、ＬＡＮ（Local Area Network）、ＷＡＮ（Wide Area Network）等を用いてもよい。また、携帯端末からのアクセス時は、移動体通信網を介してネットワーク９０へと接続される。
【００１６】認証サイト２０において、ユーザ情報データベース４は、各提携サイト５０～５２で用いる認証情報（ＩＤ、パスワード）を含むユーザ情報を記憶する。図２は、ユーザ情報のデータ構成を示す図である。この図において、ユーザ情報は、それぞれユーザ名、クレジットカード番号、上記認証情報（ＩＤ、パスワード）、ニックネーム（呼称情報）の各フィールドからなる。ここで、ユーザ名はこのユーザの氏名であり、ニックネームはこのユーザを各提携サイト上で表示させるためのものである。
【００１７】次に、図３を参照して、ユーザが認証サイトから認証情報の発行を受ける処理フローを説明する。この図において、まずユーザは、ユーザ端末７０からＵＲＬ（Uniform Resource Locator）を指定して認証サイト２０にアクセスする。そして、自己のクレジットカード番号を入力して認証情報の発行を要求する（ステップＳ１００）。この際、ユーザの属性情報（氏名、住所、電話番号等）も入力してもよい。認証サイト２０の制御手段２は、受信したクレジットカード番号（ユーザ属性情報を含んでもよい）をクレジットカード管理会社３０へ送信する（ステップＳ２００）。
【００１８】クレジットカード管理会社３０は、受信したクレジットカード番号が、管理されているクレジットカード番号に一致するかの認証処理を行い（ステップＳ３００）、認証結果を送信する（ステップＳ３０２）。認証処理において、クレジットカード番号の他、ユーザ属性情報を管理データと照合するようにしてもよい。
【００１９】制御手段２は、認証成立の結果を受信した場合に、このユーザに対して上記ＩＤ及びパスワードを発行し、ユーザ端末７０に送信する（ステップＳ２０２、Ｓ２０４）。なお、認証不成立の結果を受信した場合は、ＩＤ及びパスワードを発行せず、不成立の旨をユーザ端末に送信する。
【００２０】また、制御手段２は、ニックネームの入力を要求する（ステップＳ２０６）。この入力要求は、所定の入力ページをユーザ端末に送信することで行う。これに対し、ユーザは、ユーザ端末から所望のニックネームを入力して送信する（ステップＳ１０２）。制御手段２は、受信したニックネームを上記ＩＤ及びパスワードに関連付けてユーザ情報ＤＢ４に格納する（ステップＳ２０８）。なお、以上の処理においては、クレジットカード番号のネットワークからの漏洩を防止するため、適宜所定のセキュリティ技術を用いて送受信するようにするとよい。
【００２１】次に、図４を参照して、ユーザが提携サイトへアクセスする処理フローを説明する。この図において、まずユーザは、ユーザ端末７０から所定のＵＲＬを指定して提携サイト５０にアクセスし、上記ＩＤ及びパスワードを入力する（ステップＳ１１０）。提携サイト５０は、受信したＩＤ及びパスワードを認証サイト２０へ送信して認証を依頼する（ステップＳ２１０）。認証サイト２０の制御手段２は、受信したＩＤ及びパスワードをユーザ情報ＤＢ４に記録されたデータと照合して認証処理をする（ステップＳ３１０）。また、認証が成立した場合、制御手段２は、このＩＤ及びパスワードに対応するユーザのニックネームをユーザ情報ＤＢ４から読み出し、認証結果とニックネームを提携サイト５０へ送信する（ステップＳ３１２）。なお、認証不成立の場合、ニックネームの読み出しはせず、不成立の旨を提携サイトに送信する。
【００２２】提携サイト５０は、認証成立の旨を受信すると、アクセス制限していた機能を、このユーザ端末に対して許容する処理を行う。ここで、アクセス制限機能の許容とは、例えば所定のＷｅｂページをユーザ端末に送信することの禁止や、ユーザ端末からの入力を受け付

けることの禁止を解除することである。また、提携サイト５０は、受信したニックネームを適宜記録し（ステップＳ２１２）、認証結果とニックネームをユーザ端末に送信する（ステップＳ２１４）。ユーザは、アクセス制限のあるＷｅｂページの閲覧要求をユーザ端末から送信し（ステップＳ１１２）、提携サイト５０はユーザ端末にこのＷｅｂページを送信する（ステップＳ２１６）。ユーザはユーザ端末を介してＷｅｂページを閲覧し（ステップＳ１１４）、必要に応じてニックネームを入力する（ステップＳ１１６）。ニックネーム入力は、例えばＢＢＳ（電子掲示板システム）に投稿する場合のユーザ表示の際に行う。なお、認証成立の旨の代わりに、ニックネームを受信したことに基づき、提携サイト５０がアクセス制限していた機能を許容するようにしてもよい。

【００２３】提携サイト５０は、受信したニックネームとステップＳ２１２で記録されたニックネームとの照合を行い（ステップＳ２１８）、照合成立の場合、ニックネームの表示処理を行う（ステップＳ２２０）。このようにすると、各ユーザに割当てられたニックネーム以外の呼称が提携サイト５０上で使用（表示）されることがなく、各ユーザは自己のニックネームをユニークにサイト上で使用できることになる。つまり、正規のユーザ以外が同一ニックネームを使用することが防止される。なお、上記ステップＳ２１２、２１８の処理は必須ではなく、入力されたニックネームを直ちに表示処理しても勿論よい。

【００２４】一方、（認証サイト２０の）制御手段２は、提携サイト５０からステップＳ２１０で認証依頼がされる毎に、課金情報を課金ＤＢ６に記録する（ステップＳ３１４）。この課金情報に基づき、提携サイトに対して認証費用の請求がされることになる。

【００２５】なお、別の提携サイト５０あるいは５２にアクセスする場合、ユーザ端末は、ステップＳ１１０以降の処理を再度行う。つまり、提携サイトへアクセスする毎に認証処理を行うことになる。

【００２６】図５は、上記図４のフローに従って、ユーザ端末に表示される画面の遷移例を示す。ユーザはＬｏｇｉｎ画面１０００にて、テキストボックス１０００ａ、１０００ｂにそれぞれＩＤ，パスワードを入力する（図５（１）、ステップＳ１１０に相当）。認証が成立すると、その旨の画面１１００が表示され、また、このユーザが使用可能なニックネーム「あおのり」が表示欄１１００ａに表示される（図５（２））。認証成立により、ユーザはアクセス許容されたＷｅｂページ画面１２００を閲覧する（図５（３））。また、ＢＢＳ画面１３００では、投稿ユーザのニックネーム、及び投稿内容が表示欄１３００ａ、１３００ｂにそれぞれ表示される（図５（４））。ここで、上記したステップＳ２１８の処理がされていれば、表示欄１３００ａに同一ニックネームが重複表示されることがなく、各ユーザは自分に割当てられたニックネームをユニークに使用できる。

【００２７】本発明は上記した実施形態に限られない。例えば、ニックネームの登録をせず、提携サイトでは認証情報によるユーザの認証のみを行うようにしてもよい。また、クレジットカードの有効期間等に応じてクレジットカード管理会社が管理するデータは適宜変更される。従って、ユーザ情報ＤＢに格納されたクレジットカード番号を、上記管理データに従って更新するようにしてもよい。この更新は、クレジットカード管理会社からの指示によって行ってもよく、また、所定の時期に認証サイトからクレジットカード管理会社に問い合わせをしてもよい。また、ユーザに対するクレジットカード発行が禁止された場合は、ユーザ情報ＤＢに格納されたユーザ情報を削除することで、提携サイトへのアクセスを拒否できる。

【００２８】さらには、提携サイトごとに別の認証情報を発行し、格納するようにしてもよい。そして、提携サイトからの認証依頼が成立する毎に、認証システムで新規にユーザの呼称情報を生成して送信してもよい。この場合、提携サイトで認証がされる度に、ユーザは新たなニックネームを使用することになる。

【００２９】なお、本発明の認証システムは、コンピューターと、通信装置等の各種周辺機器と、そのコンピューターによって実行されるソフトウェアプログラムとによって実現することができ、上記システム内で実行されるソフトウェアプログラムは、コンピューター読み取り可能な記憶媒体あるいは通信回線を介して配布することが可能である。

【００３０】

【発明の効果】以上説明したように、本発明によれば、ユーザの提携サイトへのアクセス許否の判断を、当該提携サイトの代わりに認証システムで行うので、提携サイトは認証処理の負担が軽減される。

【００３１】また、請求項２記載の本発明によれば、認証がされたユーザの呼称情報を提携サイトへ送信するので、ユーザは提携サイト上でこの呼称情報を閲覧し、適宜当該提携サイト上で使用（表示）することができる。特に、ユーザの氏名等の個人情報の送信は安全上や法律上問題となることがあるが、呼称情報であればかかる問題がないという利点がある。請求項３記載の本発明によれば、認証システムでは予めユーザのクレジットカード番号に基づいた認証情報を発行しているので、クレジットカードの発行を受けている優良・安全なユーザのみが提携サイトへアクセス許容される。従って、提携サイトにおいては、不特定多数のユーザによる不正行為等の発生を有効に防止できる。請求項４記載の本発明によれば、提携サイトからの認証依頼に対して課金するので、提携サイトへ認証費用を適宜請求できる。

【図面の簡単な説明】

【図１】　本発明の認証システムの構成を示すブロック

図である。

【図２】　ユーザ情報のデータ構成を示す図である。

【図３】　ユーザが認証サイトから認証情報の発行を受ける処理フローを示す図である。

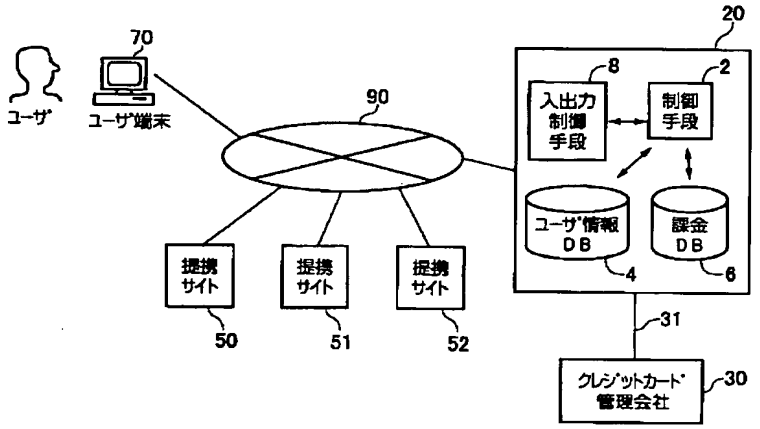
【図４】　ユーザが提携サイトへアクセスする処理フローを示す図である。

【図５】　ユーザ端末の表示される画面の遷移例を示す図である。

【符号の説明】

2	制御手段
4	ユーザ情報データベース（ＤＢ）
２０	認証システム
５０～５２	提携サイト
７０	ユーザ端末
９０	ネットワーク

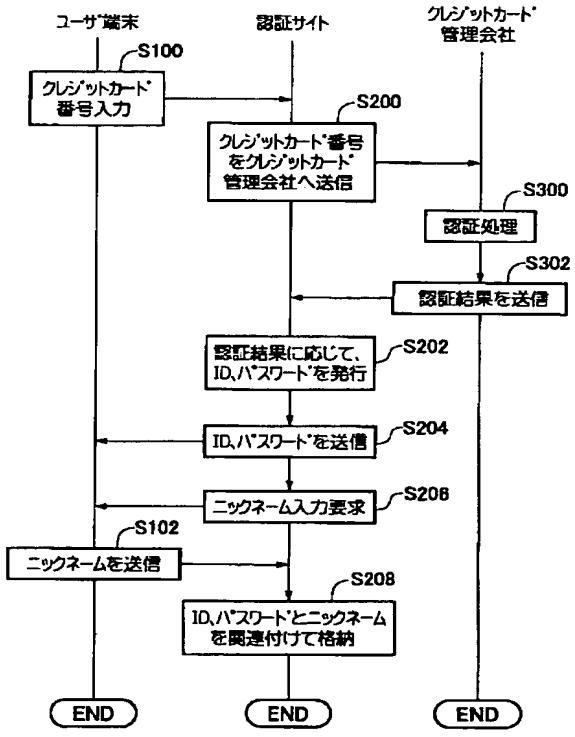
【図１】



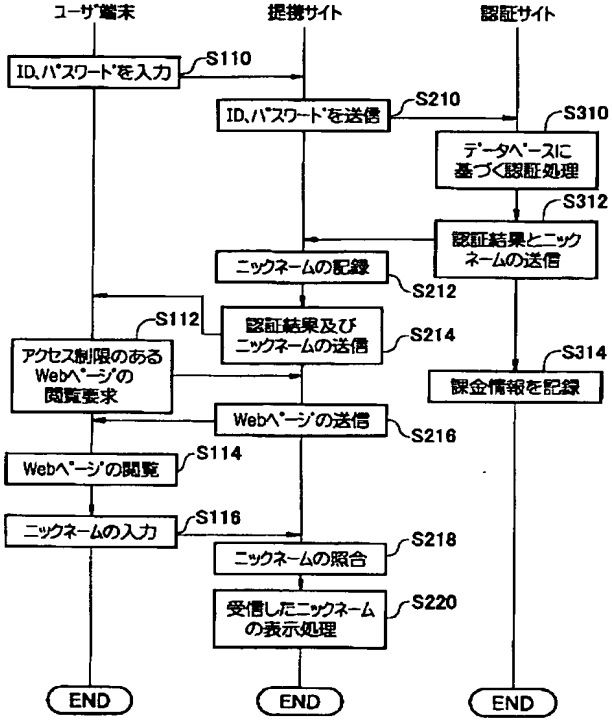
【図２】

ユーザ名	クレジットカード番号	ID	パスワード	ニックネーム
青木××	・・・・・・・	○○×	△△△△	あおのり

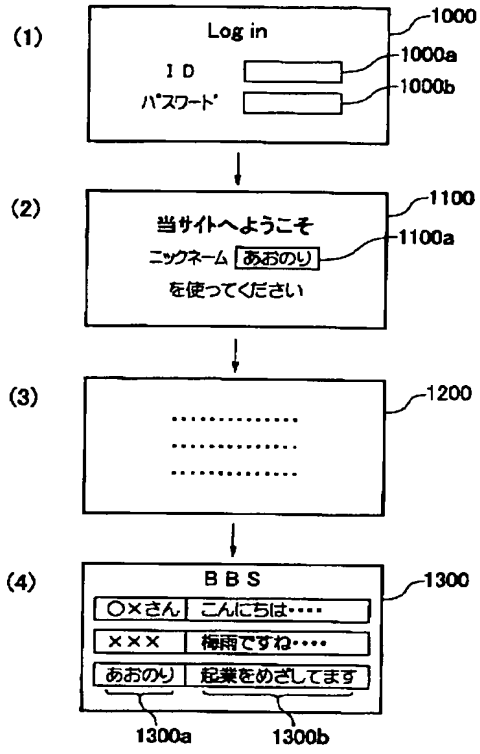
【図３】



【図４】


ユーザ端末
提携サイト
認証サイト
ID、パスワードを入力
S110
ID、パスワードを送信
S210
S310
データベースに基づく認証処理
S312
認証結果とニックネームの送信
ニックネームの記録
S212
S112
認証結果及びニックネームの送信
S214
S314
アクセス制限のあるWebページの閲覧要求
課金情報を記録
Webページの送信
S216
Webページの閲覧
S114
ニックネームの入力
S116
ニックネームの照合
S218
受信したニックネームの表示処理
S220
END
END
END

【図５】


(1)
Log in
ＩＤ
パスワード
1000
1000a
1000b
(2)
当サイトへようこそ
ニックネーム
あおのり
を使ってください
1100
1100a
(3)
1200
(4)
ＢＢＳ
○×さん
こんにちは・・・・
×××
梅雨ですね・・・・
あおのり
起業をめざしてます
1300
1300a
1300b